China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions

recordedfuture.com/redecho-targeting-indian-power-sector/

Blog

Posted: 28th February 2021

By: INSIKT GROUP

Insikt Group

***Editor's Note**: The following post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*

This report details a campaign conducted by a China-linked threat activity group, RedEcho, targeting the Indian power sector. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis. Data sources include the Recorded Future Platform, SecurityTrails, Spur, Farsight, and common open-source tools and techniques. The report will be of most interest to individuals engaged in strategic and operational intelligence relating to Indian and Chinese activity in cyberspace.

Recorded Future notified the appropriate Indian government departments prior to publication of the suspected intrusions to support incident response and remediation investigations within the impacted organizations.

Executive Summary

Relations between India and China have deteriorated significantly following border clashes in May 2020 that resulted in the first combat deaths in 45 years between the world's two most populous nations. As a result, on January 12, 2021, India's foreign minister Subrahmanyam Jaishankar announced that trust

between India and China was “profoundly disturbed.” While diplomacy and economic factors have been effective in preventing a full-blown war, notable most recently with the bilateral disengagement at the border, cyber operations continue to provide countries with a potent asymmetric capability to conduct espionage or pre-position within networks for potentially disruptive reasons.

Since early 2020, Recorded Future’s Insikt Group observed a large increase in suspected targeted intrusion activity against Indian organizations from Chinese state-sponsored groups. From mid-2020 onwards, Recorded Future’s midpoint collection revealed a steep rise in the use of infrastructure tracked as AXIOMATICASYMPTOTE, which encompasses ShadowPad command and control (C2) servers, to target a large swathe of India’s power sector. 10 distinct Indian power sector organizations, including 4 of the 5 Regional Load Despatch Centres (RLDC) responsible for operation of the power grid through balancing electricity supply and demand, have been identified as targets in a concerted campaign against India’s critical infrastructure. Other targets identified included 2 Indian seaports.

Using a combination of proactive adversary infrastructure detections, domain analysis, and Recorded Future Network Traffic Analysis, we have determined that a subset of these AXIOMATICASYMPTOTE servers share some common infrastructure tactics, techniques, and procedures (TTPs) with several previously reported Chinese state-sponsored groups, including APT41 and Tonto Team.

Despite some overlaps with previous groups, Insikt Group does not currently believe there is enough evidence to firmly attribute the activity in this particular campaign to an existing public group and therefore continue to track it as a closely related but distinct activity group, RedEcho.

Key Judgements

- The targeting of Indian critical infrastructure offers limited economic espionage opportunities; however, we assess they pose significant concerns over potential pre-positioning of network access to support Chinese strategic objectives.
- Pre-positioning on energy assets may support several potential outcomes, including geo-strategic signaling during heightened bilateral tensions, supporting influence operations, or as a precursor to kinetic escalation.
- RedEcho has strong infrastructure and victimology overlaps with Chinese groups APT41/Barium and Tonto Team, while ShadowPad is used by at least 5 distinct Chinese groups.

- The high concentration of IPs resolving to Indian critical infrastructure entities communicating over several months with a distinct subset of AXIOMATICASYMPTOTE servers used by RedEcho indicate a targeted campaign, with little evidence of wider targeting in Recorded Future's network telemetry.

***Editor's Note**: This post was an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*